CIAM schützt Daten und Kunden

Zusätzliche Sicherheitsschicht durch Customer-/Consumer-Identity- und -Access-Management

Der Durchgriff von Apps und Web-Services auf Kundendaten im Backend ist eine heikle Sache – Gleiches gilt für die Authentifizierung solcher Anfragen. Lösungen zum Customer-/Consumer-Identity- und -Access-Management (CIAM) können hier gleichzeitig Sicherheit, Usability und Marketing dienlich sein.

Von Stephan Schweizer, Zürich

Die digitale Transformation sowie die EU-Datenschutzgrundverordnung (DS-GVO) erhöhen zukünftig noch die Anforderungen an den Schutz geschäftlicher und personenbezogener Daten, wie sie in Backendsystemen vorliegen, für die über (Web-)Frontends oder Apps heute häufig auch ein breiter Zugriff durch Kunden oder Partner notwendig ist. Ein Customer-/Consumer-Identity- und -Access-Management (CIAM) kann hier als übergeordnete Instanz dienen, welche die Korrelation und Zusammenführung von Kundendaten ermöglicht (vgl. Abb. 1) und gleichzeitig eine zusätzliche Sicherungsschicht zwischen die Clients und Datenbanken im Backend einzieht (vgl. Abb. 2).

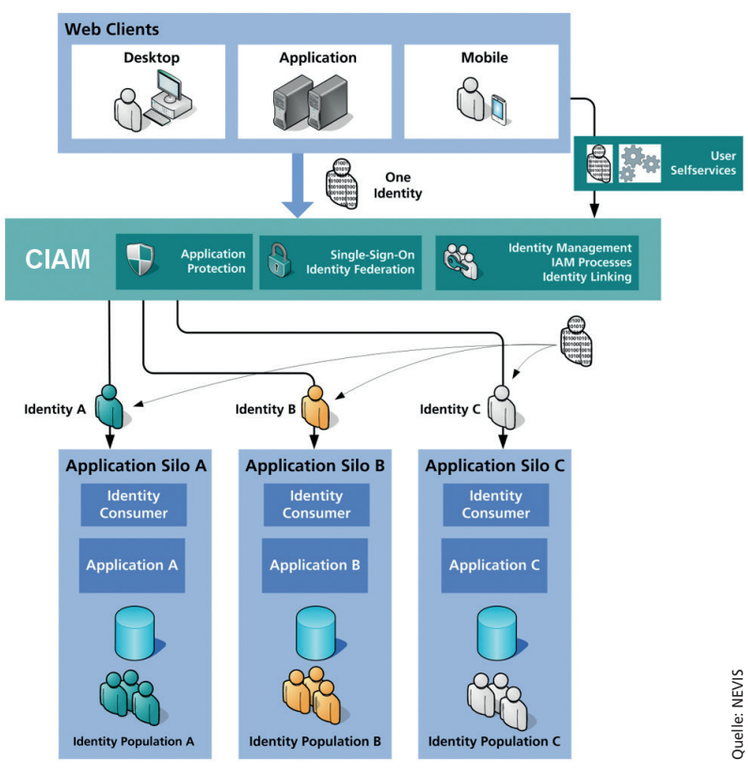

Abbildung 1: Zusammenführung verschiedener Identity-Silos in einem vorgelagerten Consumer-Identity- und -Access-Management (CIAM)

Quelle: NEVIS

Einmal etabliert, eröffnet ein CIAM-System eine Vielzahl weiterer Möglichkeiten: Um den administrativen Aufwand zu reduzieren, können Kunden unter gewissen Vorbedingungen (z. B. Zwei-Faktor-Authentifizierung) Self-Services zur Verwaltung der eigenen Daten zur Verfügung gestellt werden. Damit lässt sich auch bereits das „Recht auf Auskunft" der DS-GVO erfüllen, sofern Kunden hierüber Einblick auf die aggregierten eigenen Daten erhalten, zu denen selbstverständlich auch die durch den Benutzer erteilten, kontextspezifischen Freigaben zur Datenhaltung gehören. Ein modernes CIAM-System enthält alle notwendigen Elemente, um solche Freigaben vom Benutzer zu erhalten und zu verwalten. Auch auf der Seite der innerbetrieblichen Abläufe, des Partner- und Endkundenmarketings sowie bei der Entwicklung neuer Geschäftsfelder ist ein vereinheitlichtes System der Kundendatenverwaltung von großem Vorteil.

Allerdings muss man sicherstellen, dass nur solche Mitarbeiter und Systeme auf Kundendaten Zugriff haben, die das aufgrund ihrer Tätigkeit auch benötigen (Need-to-know-Prinzip). Technisch lässt sich das mittels rollenbasierter Zuweisungen von Elementarrechten realisieren, die ein CIAM für Mitarbeiter

solche Fragen kann es policygesteuert entscheiden, wie mit einer Anfrage weiter verfahren werden soll.

Falls beispielsweise alle Kontext-Attribute darauf hindeuten, dass es sich um einen bekannten, legitimen Benutzer handelt, so kann auch zusätzlicher Komfort gewährt werden, indem das System beispielsweise auf eine Zwei-Faktor-Authentifizierung verzichtet.

Auf der anderen Seite können das Benutzerverhalten sowie relevante Kontext-Attribute auch als Warnsignale dienen, etwa:

- ein Gerätewechsel während einer Sitzung,
- ein stark vom Üblichen abweichender oder während der Sitzung veränderter Standort,
- unnatürliche oder untypische Eingaben oder
- andere atypische Handlungen.

Die verschiedenen Signale kann ein CIAM-System zu einem „Risk-Score" konsolidieren, der während einer laufenden Sitzung kontinuierlich aktualisiert wird. Überschreitet er ein bestimmtes Maß, kann policygesteuert entschieden werden, wie mit der Sitzung zu verfahren ist. Denkbar sind zusätzliche Authentifizierungsschritte, eine Benachrichtigung des Benutzers über einen separaten Kanal (z. B. Push-Notification) oder auch ein Abbruch der Session.

Dieses „Progressive Profiling", also die fortwährende Beobachtung von Nutzerverhalten und Datentransfer, ist dabei nicht nur aus Security-Sicht hilfreich: So erlangt ein Unternehmen gleichzeitig eine konsolidierte Datensicht auf seine Kunden. Falls der Kunde seine Einwilligung dazu gibt, eröffnet dieses verbesserte Verständnis zu den Kundenbedürfnissen auch im Marketing neue automatisierbare Wege.

Tipps fürs CIAM-Projekt

Viele Unternehmen, welche die Einführung einer CIAM-Lösung planen, müssen deren Interoperabilität über Netzwerk- und Unternehmensgrenzen hinweg sicherstellen. In der Regel sind dabei sowohl On-Premise-Systeme als auch Systeme bei Partnern sowie Cloud-Applikationen zu einem Gesamtsystem zu integrieren. Die Basis dafür ist die Nutzung offener Standards wie OAuth2, OpenID Connect oder SAML. Gleichzeitig bedeutet die Aufweichung von Unternehmensgrenzen höhere Anforderungen an die Sicherheit. Projekte solchen Umfangs lassen sich am besten unter früher Einbeziehung eines CIAM-Anbieters angehen, idealerweise bereits in der Konzeptphase.

Wichtig ist zudem, dass ein CIAM-Projekt gut mit der Business-Organisation auf Kundenseite abgestimmt wird. Dazu sollte man unter Einbezug der kundenseitigen Business-Organisation sowie der IT die Use-Cases und User-Journeys in gemeinsamen Workshops definieren und priorisieren.

Anhand dieser Priorisierung lässt sich das CIAM-System dann schrittweise aufbauen und parametrisieren. Erste Tests sind bereits in einer frühen Phase empfehlenswert:

- Integrationstests mit den Entwicklern der Services
- Sicherheitsscans
- Tests zu Ausfallsicherheit und Business-Continuity
- Tests zur Akzeptanz durch die Endanwender

Abhängig von der Ausgangslage sowie der bestehenden Systemlandschaft folgen dann vor der Inbetriebnahme die weiteren Schritte:

- Bestehende Identitäts-Silos werden schrittweise aufgelöst und in die zentrale CIAM-Umgebung integriert.
- Parallel dazu erfolgt die Integration der zugehörigen Applikationen.
- Mit der Integration der Applikationen im zweiten Schritt kommen Benutzer, die mehrere Anwendungen nutzen, bereits in den Genuss eines applikationsübergreifenden Single-Sign-ons (SSO). Die Steuerung, welche Applikationen dem jeweiligen Benutzer zur Verfügung stehen, erfolgt dabei idealerweise über Rollen, die den Benutzern im Rahmen der OnBoarding- und Self-Service-Prozesse zugeordnet werden.
- Parallel zur Inbetriebnahme der neuen Identity-Management-Prozesse muss eine Schulung für Helpdesk- und Support-Mitarbeiter erfolgen.
- Weitere Benutzergruppen und Anwendungen werden dann im Ein- bis Zwei-Monats-Rhythmus integriert.

Fazit

Die strengen Anforderungen der DS-GVO werden in vielen Unternehmen als große Belastung wahrgenommen – doch die Verordnung kann auch als Katalysator dienen, um das Vertrauen der Kunden in die Sicherheit der angebotenen Services zu stärken. Umfragen belegen, dass das Thema Sicherheit bei der Auswahl von Anbietern für digitale Services eine wichtige Rolle spielt – vor allem für Services, bei denen Geld und sensitive Daten im Spiel sind.

Eine Lösung für Customer- beziehungsweise Consumer-Identity- und -Access-Management kann maßgeblich dazu beitragen, gleichzeitig die Usability für den Kunden zu verbessern, einen hohen Sicherheitsstandard zu gewährleisten und die Anforderungen der DS-GVO zu erfüllen. Damit ist der Grundstein gelegt, die Herausforderungen der Digitalisierung nicht nur erfolgreich zu meistern, sondern auch die sich bietenden Chancen für nachhaltigen Erfolg tatsächlich zu nutzen. ■

Stephan Schweizer ist „Chief Product Officer NEVIS" bei der AdNovum Informatik AG.